

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Virginia

In the Matter of the Search of )

(Briefly describe the property to be searched or identify the person  
by name and address)

Case No. 1:24-SW-592

UNDER SEALINFORMATION ASSOCIATED WITH NAME USER )  
IDENTIFICATION NUMBER 1142201852792934541 )  
STORED AT PREMISES CONTROLLED BY DISCORD, )  
INC. )**WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS**

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Northern District of California  
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

SEE ATTACHMENT B

**YOU ARE COMMANDED** to execute this warrant on or before August 30, 2024 (not to exceed 14 days)☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.


The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Ivan D. Davis

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)☐ for      days (not to exceed 30) ☐ until, the facts justifying, the later specific date of     Date and time issued: 08/16/2024 1:30 pm

Digitally signed by Ivan Davis

Date: 2024.08.16 14:40:08 -04'00'

  
Judge's signatureCity and state: Alexandria, VirginiaHon. Ivan D. Davis, United States Magistrate Judge

Printed name and title



**Return**

Case No.:

1:24-SW-592

Date and time warrant executed:

08/19/2024 @ 8:31 PM

Copy of warrant and inventory left with:

N/A

Inventory made in the presence of:

N/A

Inventory of the property taken and name(s) of any person(s) seized:

(1) zip file containing digital content/attachments from Discord Inc. pertaining to user ID 1142201852792934541.

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 09/23/2024



Executing officer's signature

Olivia Temowski / Special Agent

Printed name and title



## **ATTACHMENT A**

### **Property to Be Searched**

This warrant applies to information from at least May 1, 2023 until February 1, 2024 associated with the known DISCORD user Michael David Seeds, as well as information in the possession of DISCORD and associated with the following TARGET ACCOUNT:

- User identification number (UID) 1142201852792934541

This information is stored at premises owned, maintained, controlled, or operated by Discord Inc., an electronic communications service headquartered at 440 De Haro Street, Suite 200, San Francisco, CA 94107.



## **ATTACHMENT B**

### **Things to be Seized and Procedures to Facilitate Execution of the Warrant**

#### **I. Information to be Disclosed by Discord, Inc. ("DISCORD") to Facilitate Execution of the Warrant**

To the extent that the information described in Attachment A is within the possession, custody, or control of DISCORD, including any information that has been deleted but is still available to DISCORD, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), DISCORD is required to disclose the following information to the government for the TARGET ACCOUNT listed in Attachment A:

- a. All contents of all wire and electronic communications associated with the TARGET ACCOUNT for the period May 1, 2023 through February 1, 2024, including:
  - i. All e-mails, communications, or messages of any kind associated with the TARGET ACCOUNT, including stored or preserved copies of messages sent to and from the TARGET ACCOUNT, deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information associated with each e-mail or message, and any related documents or attachments;
  - ii. All records or other information stored by subscriber(s) of the TARGET ACCOUNT, including address books, voice and voice-over-IP data, contact and buddy lists, calendar data, pictures, videos, notes, texts, links, user profiles, account settings, access logs, and files;
  - iii. All records pertaining to communications between DISCORD and any person regarding the TARGET ACCOUNT, including contacts with support services and records of actions taken;



- iv. All stored passwords, including passwords stored in clear text and hash form, and for any hashed values that include a salt, DISCORD shall provide the salt value used to compute the stored password hash value, and any security questions and answers;
  - v. All search history and web history, including web clicks or “History Events,” by the user of the TARGET ACCOUNT;
  - vi. All web browsing activities that are identifiable with the TARGET ACCOUNT; and
  - vii. Any and all logs of user activity and user agent string, including: web requests or HTTP requests; any logs containing information such as the Requestor’s IP address, identity and user identification number (“UID”), date and timestamp, request URI or URL, HTTP protocol version, referrer, and other user agent string information; login tracker logs; account management logs; and any other information concerning other e-mail or social media accounts accessed or analytics related to the TARGET ACCOUNT.
- b. All other records and information, including:
- i. All subscriber information, including the date on which the TARGET ACCOUNT was created, the length of service, the IP address used to register the target account, the subscriber’s full name(s), screen name(s), any alternate names, other account names or e-mail addresses associated with the target account, linked accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers, or physical addresses, the types of service utilized,



account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, **and including any changes made to any subscriber information** or services, including specifically changes made to secondary e-mail accounts, phone numbers, passwords, identity or address information, or types of services used, and including the dates on which such changes occurred, for the following accounts:

- (1) The TARGET ACCOUNT;
  - (2) Any other account associated with the TARGET ACCOUNT, including by means of sharing a common secondary, recovery, or alternate **e-mail address listed in subscriber records** for the TARGET ACCOUNT or by means of sharing a **common phone number or SMS number listed in subscriber records** for the TARGET ACCOUNT; and
  - (3) Any other account accessed by a device with an identifier responsive to the device identifiers called for in Section I.b.iii, below.
- ii. All user connection logs and transactional information of all activity relating to the TARGET ACCOUNT described above in Section I.a, including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, and locations;
- iii. Any information identifying the device or devices used to access the TARGET ACCOUNT, including any Android ID, Advertising ID, unique application number, hardware model, operating system version, unique device identifier, Global Unique Identifier or “GUID,” serial number, mobile network



information, phone number, device serial number, MAC address, Electronic Serial Number (“ESN”), Mobile Electronic Identity Number (“MEIN”), Mobile Equipment Identifier (“MEID”), Mobile Identification Number (“MIN”), Subscriber Identity Module (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifier (“IMSI”), International Mobile Equipment Identity (“IMEI”), or Apple advertiser ID or ID for advertisers (“IDEFA”), and any other information regarding the types of devices used to access the TARGET ACCOUNT or other device-specific information; and

iv. Any information showing the location of the user of the TARGET ACCOUNT, including while sending or receiving a message using the TARGET ACCOUNT or accessing or logged into the TARGET ACCOUNT.

Within **14 days** of the issuance of this Warrant, DISCORD shall deliver the information set forth above.



## **II. Information to be Seized by the Government**

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations 18 U.S.C. §§ 2251(a)(1), 2252(a)(2) and 2252(a)(4)(B), including the following:

- a. Any messages pertaining to the production, receipt, distribution, possession, and attempt of such and access with intent to view of child pornography;
- b. All posted images and videos pertaining to the production, receipt, distribution, possession, and attempt of such and access with intent to view of child pornography;
- c. All posted text communications and public postings that further the production, receipt, distribution, possession, and attempt of such and access with intent to view of child pornography;
- d. All access logs, administrative logs, user logs and posting history that will assist in locating users;
- e. Evidence indicating how and when the SUBJECT ACCOUNT was created, accessed or used, to determine the chronological and geographical context of account access, use, and events relating to the crimes under investigation and to the SUBJECT ACCOUNT;
- f. Evidence indicating the SUBJECT ACCOUNT users' state of mind as it relates to the crimes under investigation;
- g. The identity of the person(s) who created or used the SUBJECT ACCOUNT, including records that help reveal the whereabouts of such person(s); and
- h. The identity of the person(s) who communicated with the SUBJECT ACCOUNT about matters relating to the production, receipt, distribution, possession, and



attempt of such and access with intent to view of child pornography, including records that help reveal their whereabouts.

- i. All files of child pornography and child erotica.